Preface

The September 11, 2001 terrorist attacks in the United States and the ensuing terrorist attacks around the world during 2002 underscore the international scope of the threat facing the U.S. and its allies in the War on Terrorism and the need for international cooperation to effectively address the threat.

In his preface to the U.S. Department of State report "Patterns of Global Terrorism 2001," Secretary of State Colin Powell captured the nature of the threat faced by the U.S. and indeed by all nations in this War:

> "In this global campaign against terrorism, no country has the luxury of remaining on the sidelines. There ***are*** no sidelines. Terrorists respect no limits, geographic or moral. The frontlines are everywhere and the stakes are high. Terrorism not only kills people. It also threatens democratic institutions, undermines economies, and destabilizes regions."

"There are no sidelines."

One important area in enhancing the capabilities of the U.S. and its allies in the War on Terrorism is the ability to rapidly develop and apply technology to meet the challenges posed by terrorists. In response to the threats and challenges, the Technical Support Working Group (TSWG) increased its tempo of operations and range of activities in FY 2002. For example:

- In addition to its normally scheduled Broad Agency Announcements (BAAs), the TSWG issued a BAA for the Office of the Under Secretary of Defense (Acquisition, Technology and Logistics) that resulted in 12,500 submissions from industry, academia, government, and the national laboratories. Approximately 60 of those project proposals are being funded at approximately $50 million.
- At the request of the White House Office of Science and Technology Policy, the TSWG reviewed and evaluated over 200 technical proposals submitted to the Office of Homeland Security and funded or referred the promising proposals to other agencies for funding consideration.
- The TSWG engaged the National Academies of Science to review and begin addressing long-term technology needs for combating

terrorism — an activity aligned with TSWG's objective of influencing long-term research and development.

- The TSWG expanded its international cooperative activities in the form of increased, but very focused, program activity with its current international partners and began discussions with two other nations that may lead to additional technology agreements to combat terrorism.

The importance of allied cooperation and support for the War on Terrorism is best illustrated by the President's comments from a press briefing held on October 14, 2002 following the terrorist bombings in Bali:

> "I told…the Prime Minister of Australia and I told Prime Minister Blair this morning that I'm absolutely determined to continue to lead the coalition. They recognize the need for us to continue to work together. And it's a sad day for a lot of people around the world…but it also is a day in which we've got to realize that we've got a long way to go to make the world more secure and more peaceful."

In furtherance of our national goals, the TSWG is continuing to focus its program development efforts to balance investments across the four pillars of combating terrorism: antiterrorism; counterterrorism; intelligence support; and consequence management. The challenge is to provide a coherent and consistent context for technology development based upon innovation, real operator needs, and proven procedures and tactics.

In this report you will read about some new capabilities developed by the TSWG in FY 2002, as well as some capabilities still under development. There are other projects which, because of sensitivity, cannot be described in an unclassified report. Together they comprise the TSWG's evolving program to develop technology and capability to support the U.S. and its allies in the War on Terrorism.

Table of Contents

TSWG Organization

In April 1982, National Security Decision Directive (NSDD) 30 assigned responsibility for the development of overall U.S. policy on terrorism to the Interdepartmental Working Group on Terrorism (IG/T) chaired by the Department of State (DOS). The TSWG was an original subgroup of the IG/T, which later became the Interagency Working Group on Counterterrorism. In its February 1986 report, a cabinet level Task Force on Counterterrorism led by then Vice-President Bush cited the TSWG as assuring "the development of appropriate counterterrorism technological efforts."

Today, TSWG still performs that counterterrorism technology development function as a stand-alone interagency working group. TSWG's mission is to conduct the national interagency research and development (R&D) program for combating terrorism requirements. It also has commenced efforts to conduct and influence longer-term R&D initiatives and, reflecting the shift to a more offensive strategy, balance its technology and capability development efforts among the four pillars of combating terrorism: intelligence support; counterterrorism; antiterrorism; and consequence management.

Structure

TSWG operates under the policy oversight of the Department of State's Coordinator for Counterterrorism and the management and technical oversight of the Department of Defense (DoD) Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (ASD (SO/LIC)). Participation is open to federal departments and agencies. While the TSWG's core funds are derived principally from the DoD's Combating Terrorism Technology Support (CTTS) Program, and the DOS, other departments and agencies contribute additional funds. Other departments and agencies also provide personnel to act as project managers and technical advisors.

As a result of Congressional direction for the TSWG to engage in joint counterterrorism R&D efforts with selected NATO and major non-NATO allies, the TSWG assumed an international dimension in FY 1993. TSWG conducts cooperative R&D with the United Kingdom, Canada, and Israel through separate bilateral agreements.

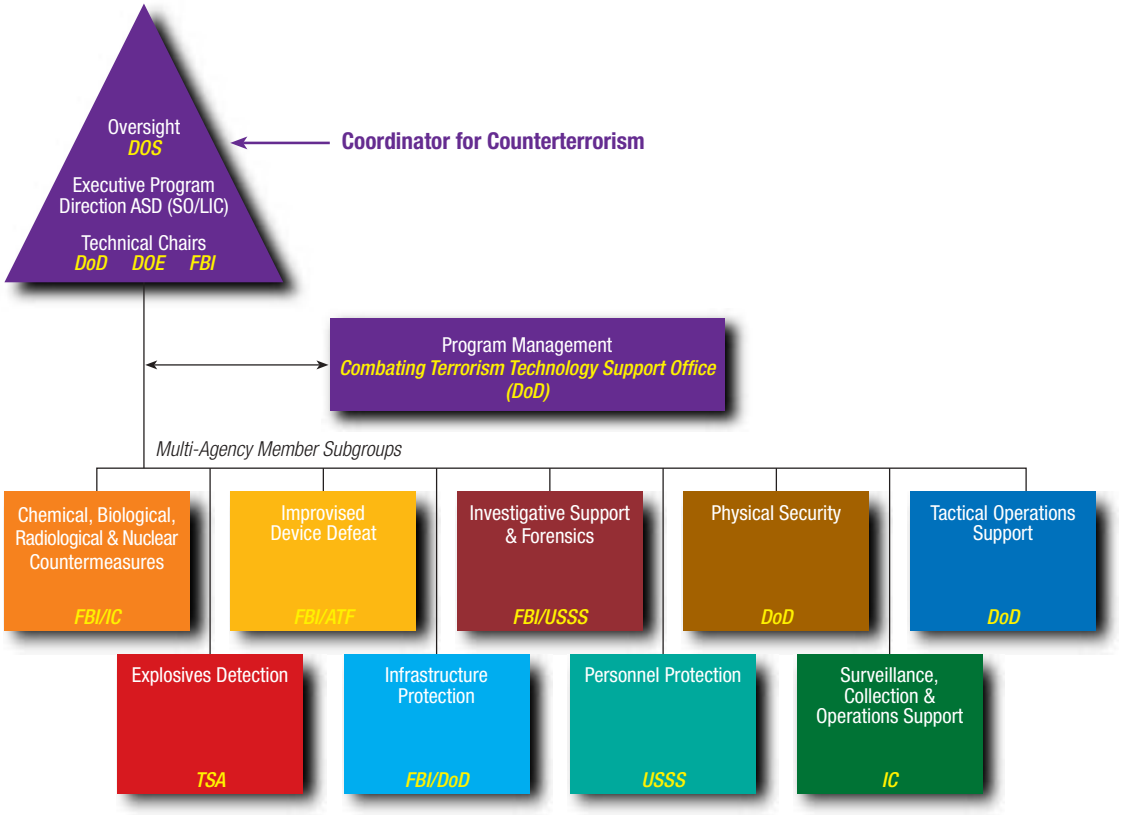
The TSWG has successfully transitioned capabilities to the Departments of Agriculture, Defense, Justice, State, and Treasury (Secret Service, Customs, and the Bureau of Alcohol, Tobacco, and Firearms); the Intelligence Community; the Transportation Security Administration; the Public Health Service; and other departments and agencies.

TSWG membership includes representatives from over eighty organizations across the Federal Government. These departments and agencies work together by participating in one or more subgroups. A comprehensive listing of member organizations by subgroup is provided in the appendix.

The nine subgroups are: Chemical, Biological, Radiological and Nuclear Countermeasures; Explosives Detection; Improvised Device Defeat; Infrastructure Protection; Investigative Support and Forensics; Personnel Protection; Physical Security; Surveillance, Collection and Operations Support; and Tactical Operations Support.

In FY 2002, the Explosives Detection and Defeat Subgroup was divided into two subgroups: Explosives Detection and Improvised Device Defeat. This change improved the focus on both of these important areas.

TSWG Organization

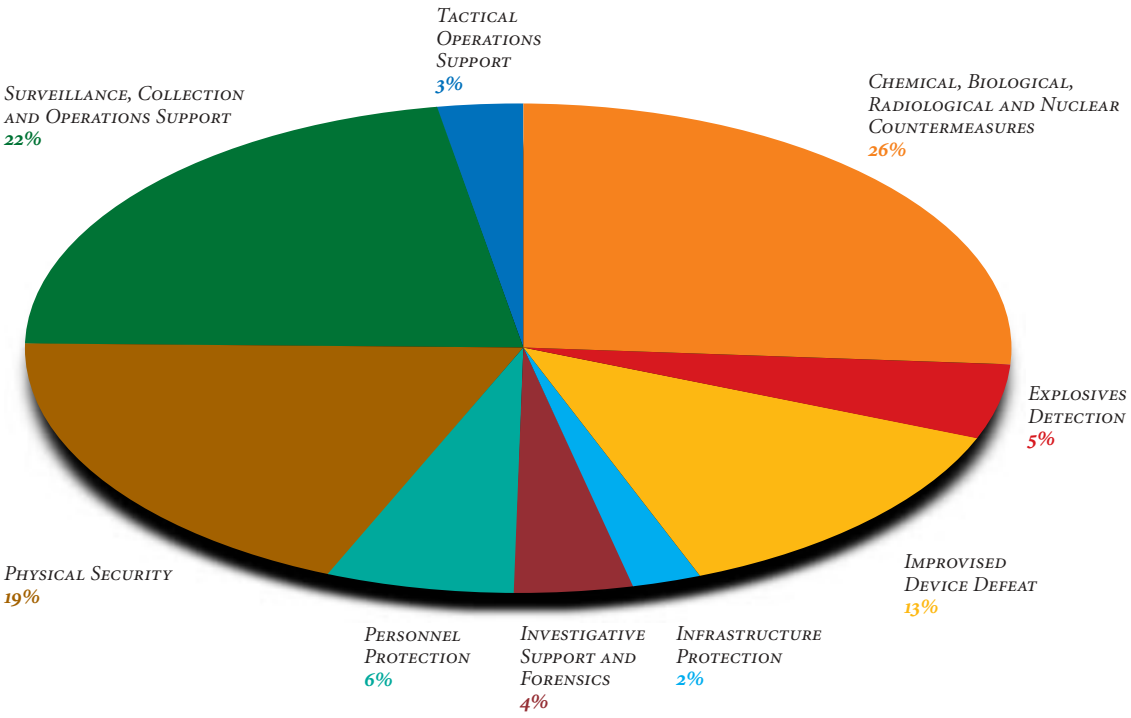


Each Subgroup is chaired by a senior representative from a Federal agency with special expertise in that functional area. Chairmanship of four Subgroups is shared as indicated in the organizational chart above.

TSWG Program Funding

Funding for the TSWG program has increased from $8 million in FY 1992 to approximately $111 million in FY 2002. This increase reflects the concern over terrorist activity and the recognized need to accelerate the development of technology to effectively address the threat. The Department of Defense provides the bulk of funding for TSWG activities. The Department of State contributes annually to TSWG core funding, while other departments and agencies share the costs of selected projects.

TSWG FY 2002 Program Funding *($111 Million)*



Chemical, Biological, Radiological and Nuclear Countermeasures

Mission

Identify and prioritize interagency chemical, biological, radiological and nuclear combating terrorism requirements and deliver technology solutions for detection, protection, decontamination, mitigation, containment and disposal.

The Chemical, Biological, Radiological and Nuclear (CBRN) Countermeasures Subgroup identifies and prioritizes interagency user requirements for countering terrorist employment of CBRN materials. Through its participation in the InterAgency Board (IAB) for Equipment Standardization and InterOperability, and in coordination with the NIJ, FEMA, EPA and OHS, the subgroup addresses technology requirements from the fire, hazardous materials, law enforcement, and emergency medical services communities. The subgroup co-chairs are from the FBI Hazardous Materials Response Unit (HMRU) and the Intelligence Community. They ensure a balanced program that addresses both domestic and foreign CBRN threats.

Focus Areas

The CBRN Countermeasures Subgroup focus areas reflect the prioritized requirements of the CBRN response community. During FY 2002, the TSWG CBRN Countermeasures Subgroup focused on the following areas:

Detection

Improve the sampling, detection, and forensic analysis of food- and water-borne CB agents, toxic industrial chemicals, low-concentration chemical warfare agents and biological warfare agents.

Protection

Improve the operating performance and decrease the cost of personnel and building protection equipment. Tasks include developing protective masks that can be quickly donned during escapes from CBRN incident areas, equipment that will protect building occupants from attack, and expanding protection against toxic industrial chemicals.

Decontamination

Develop technologies and protocols for personnel, facilities and equipment decontamination. Systems will be low-cost, environmentally-benign, safe, and effective at decontaminating biological and chemical warfare agents and persistent toxic industrial chemicals.

Membership

- Amtrak Police Department
- Environmental Protection Agency
- Federal Emergency Management Agency
- General Services Administration
  FPS
- InterAgency Board
- Intelligence Community
- Metro Transit Police Department
- Nuclear Regulatory Commission
- U.S. Capitol Police
- U.S. Department of Agriculture
  APHIS, ARS, FSIS, OIG
- U.S. Department of Commerce
  NIST
- U.S. Department of Defense
  ACC, AMRIID, BCJOC, CBIRF, CENTCOM, DARPA, DIA, DPS, DTRA, ECBC, ESC, FPBL, 52nd Ord, FORSCOM, JCS, MANSCEN, NAVCENT, NAVEODTECHDIV, NAWC, NGIC, NSA, NSWC, OATSD/CBD, ONR, SBCCOM, SG, SOCOM, TEU, USACMLS
- U.S. Department of Energy
  CBNP, OS
- U.S. Department of Health and Human Services
  CDC, FDA, OEP, USPHS
- U.S. Department of Justice
  FBI-BDC, -HMRU, -WMDOU; NIJ, USMS
- U.S. Department of State
  DS, OBO, S/CT
- U.S. Department of Transportation
  TSA, USCG
- U.S. Department of the Treasury
  USCS, USSS-TSD
- U.S. Postal Inspection Service
- White House
  OHS, OSTP

Training

Develop hardware and software for military and civilian CBRN Consequence Management training. Training materials will employ Advanced Distance Learning media, including web-based information, interactive CD-ROM software, and virtual reality simulation access via the Internet.

Information Resources

Develop shared information management tools that provide a common "picture of the incident" and facilitate the efficient integration of diverse emergency and consequence management elements from federal, state and local agencies.

Selected Completed Projects

CBR Counter Terrorism (CT) Simulant Training Kit

The CBR CT Simulant Training Kit was developed to assist security personnel in recognizing improvised chemical, biological, and radiological materials. The kit provides visual and odor simulants for select improvised CBR materials. The included user manual provides detailed information on the materials and notes the differences in physical properties and appearance that might exist between military grade and low purity materials. The kit is available to all federal, state and local public safety and security agencies.

Mass Personnel Decontamination Protocols

A terrorist release of hazardous chemical or biological materials in an urban environment against a civilian population presents unique decontamination challenges that are not adequately addressed through existing personnel decontamination procedures. The technical validity and operational desirability of existing procedures were evaluated and evidence- and consensus-based guidelines and best practices for decontaminating civilian populations in the event of a CB incident were developed. These protocols were developed in cooperation with the United Kingdom, Canada and Australia.

Biological Swab Sampler

One of the greatest challenges facing current responders is to effectively and reproducibly sample contaminated surfaces in office buildings where bioterrorism is suspected. After collection, the sample is transferred to a biological detection capability. Swab performance against spore-forming and vegetative bacteria, viruses and protein toxins was optimized. The swab sampling kit includes the swab, buffer solutions, sample vials and filters necessary to support rapid screening of the examined material. The kit is commercially available and is being used by several federal agencies.

Escape Mask Testing

The Escape Mask testing program identified the first one-size-fits-all escape mask to provide at least 15 minutes of protection against a range of threat agents. The mask can be donned in less than 30 seconds and fits easily in a desk drawer or briefcase. The Quick2000™ mask is being purchased by a number of federal agencies. Additional mask designs are being evaluated to meet the full range of capabilities needed in responding to a terrorist incident.

WMD Response Element Advanced Laboratory Integrated Training and Indoctrination (REALITI) Course

Fixed and mobile laboratories are key assets within the nation's Laboratory Response Network and are instrumental in mitigating the effects of CBR terrorist incidents. Responders, laboratory technicians and scientists within the CBRN research community require specialized skills and equipment training frequently associated with working in Chemical Surety or Biological Safety Level 3 laboratories. The WMD-REALITI course, an accredited, integrated, education and training program designed to provide users with this training, was developed. The Advanced level curriculum was completed and delivered to the National Guard Bureau.

Aerogel Sampling System

A highly porous aerogel material was integrated with selective reagents. The sampling system effectively and reproducibly collects and concentrates viral, bacterial or toxin aerosol particulates. The system is lightweight and has been operationally deployed on an unmanned aerial vehicle.

Selected Current Projects

Drink System for SCBAs and PAPRs

A universal drinking system for self-contained breathing apparatuses (SCBAs) and powered air purifying respirators (PAPRs) is being developed. This capability extends the work time of emergency personnel while responding to terrorist incidents involving chemical or biological agents. It also reduces the potential of heat stroke by ensuring proper hydration.

Electrostatic Decontamination System

A modular system consisting of a photo-activated decontamination solution, electrostatic spray applicator, and an ultraviolet (UV) light source, is being developed. The system will destroy most chemical and biological agents in under two minutes. The post-treatment residue will be environmentally benign.

WMD Panic Response Operations Course

Differentiating between valid stress reactions and psychosomatic disorders in the wake of a WMD incident proves very challenging for emergency responders. A course is being developed that will focus on the effects of fear of the unknown, the inducement of mass panic, and the potential for hysteria and panic events. This course will also address the needs of laymen who provide training to civilian clinical care providers, emergency first responders, and executive level emergency managers. In addition, it will include the rudimentary functions of crowd control. Finally, the role of the media in alleviating a potential mass panic situation in a WMD event will be addressed.

Biological Threat Emergency Response System

In assessing agricultural bioterrorism threats, federal, state, and local government officials require timely access to critical information. This includes disease incidence, potential for spread, and ongoing response measures. The response system will predict, with reasonable certainty, the future spread of a disease. This system will aid in emergency management and deployment of resources.

Contact Information

cbrncsubgroup@tswg.gov

Performers

Alabama
Auburn University, Auburn

California
Lawrence Livermore National Laboratory, Livermore
Maxim Systems, Inc., San Diego
Mission Research Corporation, Santa Barbara
University of California, Davis

District of Columbia
U.S. Naval Research Laboratory

Florida
National Terrorism Preparedness Institute, St. Petersburg College, St. Petersburg
Purified Micro Environments, Orlando

Georgia
Georgia Tech Research Institute, Atlanta

Illinois
Nanosphere, Northbrook

Kansas
Midwest Research Institute, Kansas City
NanoScale Materials, Inc., Manhattan

Maryland
GEOMET Technologies, Inc., Germantown
Johns Hopkins University Medical School, Baltimore
Lagus Applied Technology, Olney
Loats Associates, Westminster
National Institute of Standards and Technology, Gaithersburg
Naval Surface Warfare Center, Carderock
Perkin-Elmer, Gaithersburg
U.S. Army Edgewood Chemical and Biological Center, Aberdeen Proving Ground
University of Maryland/Food and Drug Administration, College Park

Massachusetts
Tiax, LLC, Cambridge
Tufts University, Medford

Missouri
Clean Earth Technology, St. Louis

Nevada
University of Nevada, Las Vegas

New Jersey
Hi Temp Technology, Inc., Flemmington

New York
Veridian Pacific-Sierra Research, Buffalo

North Carolina
Research Triangle Insitute, Research Triangle
Tempest Environmental Systems, Inc., Durham

Ohio
Battelle Memorial Institute, Columbus
Komar Industries, Inc., Groveport

Pennsylvania
Carnegie Mellon University, Pittsburgh
Concurrent Technologies Corporation, Johnstown
Early Responders Distance Learning Center, St. Joseph's University, Philadelphia
Indiana University of Pennsylvania, Indiana
University of Pittsburgh, Pittsburgh

Texas
Southwest Research Institute, San Antonio
University of Texas, Austin

Utah
Mission Research Corporation, Logan
Utah State University, Logan

Virginia
Battelle Memorial Institute, Arlington
Veridian Engineering Systems, Arlington

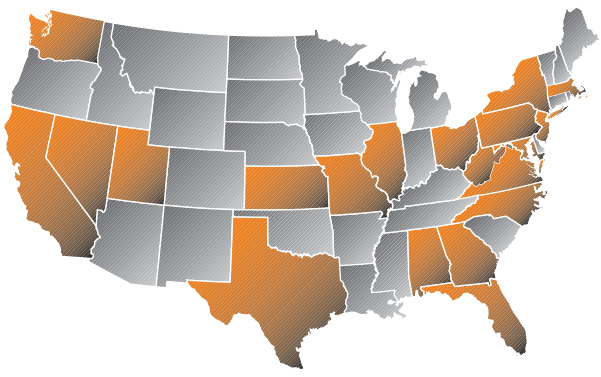
Washington
Pacific Northwest National Laboratory, Richland
Washington State University, Pullman

West Virginia
West Virginia University, Morgantown

Canada
Defence Research Establishment, Suffield

Israel
Israel Institute for Biological Research
Ministry of Defense

United Kingdom
Defence Science and Technology Laboratories



Explosives Detection

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for existing and emerging technology in the area of explosives detection and diagnostics. Emphasis is placed on a long-term, sustained approach leading to technology for detection and identification of improvised explosive devices and large vehicle bombs.

The Explosives Detection (ED) Subgroup identifies and develops technologies for detection and subsequent characterization of explosives that are concealed in packages in both bulk and trace quantities. These improvements enhance the operational capability of both military and civilian entry point screening applications. A representative from the Transportation Security Administration (TSA) chairs the subgroup.

Focus Areas

The ED Subgroup focus areas reflect the prioritized requirements of a broad range of interagency customers, including physical security and forensic analysis. During FY 2002, the TSWG ED Subgroup focused on the following areas:

Standoff Detection
Develop methods for a standoff detection capability of 100 pounds of explosives at a minimum distance of 50 feet. This includes investigating unique physical and chemical phenomena that identify the presence of explosives, the physical limits for sensor technology to respond to these phenomena, and what technology enhancements are necessary. Current standoff detection capabilities under development are limited in standoff distance and type of explosives that can be detected.

Short-range Detection and Diagnostics
Develop explosives detection and diagnostics capabilities for vehicle entry point screening and diagnostic analysis of improvised explosive devices. Areas of concern are detection rate, throughput, safety, and reliability in identification of explosives.

Marking Agents
Develop technologies that enhance manufacturing and detection techniques of marking agents currently required by law to be used in plastic explosives.

Membership

U.S. Capitol Police

U.S. Department of Defense
ACC, AFRL, DIA, DTRA, FPBL, FPSPO, JCS, NAVEODTECHDIV, NCIS, NFESC, NRL, NSA, NSWC, TEU

U.S. Department of Energy
LLNL, OS

U.S. Department of Justice
FBI-BDC, NIJ

U.S. Department of State
DS

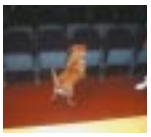
U.S. Department of Transportation
TSA, USCG

U.S. Department of the Treasury
ATF, USCS, USSS

U.S. Postal Inspection Service

Selected Completed Projects

Canine Training Aids

Non-explosive canine training aids for Comp C-4, Semtex, and nitroglycerine dynamite were developed and field-tested at several major airports. Previously, actual explosives were required to perform maintenance training of canines in the field. This caused difficulties with the transport and storage of the explosives and reduced the frequency of training. With the development of non-explosive training aids, airports will be able to safely perform much more frequent training and improve canine effectiveness.

Trace Explosives Detection Portal for Personnel Screening

A trace detection portal based on ion-mobility spectroscopy was developed jointly with TSA and forward deployed to an overseas U.S. Army facility. The portal demonstrated the ability to detect small amounts of explosives in a field environment. However, severe environmental conditions limited the operational effectiveness of the system. As a result, alternative approaches are being sought and the portal is being relocated to a less austere environment for additional field-testing.

Backscatter X-ray Portal Testing

Two different personnel screening systems using non-penetrating, backscatter x-rays were evaluated. Both systems demonstrated the ability to detect threat quantities and threat configurations of explosives. In cooperation with TSA, several systems are being forward deployed to high threat areas for additional field evaluation.

Selected Current Projects

Associated Particle Imaging

The feasibility of using associated particle imaging as a method for standoff detection of explosives is being evaluated. The ability to detect 100 pounds of certain explosives at a distance of 10 feet was demonstrated this year. Future efforts will focus on the expanding the types of explosives detected, increasing the range of detection, and reducing the size of the prototype detector equipment. A field evaluation is planned for FY 2003.

Handheld Explosives Detector

Development continues on a handheld explosives detector based on surface acoustic wave (SAW) technology. The prototype system is significantly smaller than existing explosive detection systems. This international cooperative project has demonstrated the ability to detect both triacetone triperoxide (TATP) and RDX. In FY 2003, the algorithms will be expanded to detect additional explosives and the sampling efficiency will be evaluated.

QR Personnel Screening Portal

A prototype Quadrupole Resonance (QR) portal is being developed for the detection of explosive devices concealed on personnel. Some configurations of explosives can be problematic for trace detection techniques, but are still detectable by bulk inspection methods such as QR. This effort seeks to expand the types of explosives detected by QR as well as improve the functionality of QR in personnel screening applications. Efforts have focused on demonstrating proof of principle for personnel screening applications. Work in FY 2003 will include laboratory evaluation of an advanced prototype.

Marking Agents and Low Cost Detectors

Of the four explosive marking agents ratified by the International Civil Aviation Organization and included in the 1996 Anti-Terrorism and Effective Death Penalty Act, the U.S. currently uses 2,3-dimethyl 2,3-dinotrobutane (DMNB). The cost of this material is rising and threatens to prevent many countries from being able to afford the DMNB marking agent for plastic explosives. A low cost pilot-production process for producing the marking agent was developed and tested. A full-scale production process is now being developed, which will be made available to domestic and international explosive manufacturers.

Contact Information

edsubgroup@tswg.gov

Performers

Alabama
Auburn University Institute for Biological Detection Systems, Auburn

California
Dynamics Technology Incorporated, Torrance

Quantum Magnetics, San Diego

Science Applications International Corporation (SAIC), San Diego

District of Columbia
U.S. Naval Research Laboratory

Florida
Air Force Research Lab, Tyndall AFB

Kentucky
Western Kentucky University, Bowling Green

Maryland
Naval Explosive Ordnance Disposal Technology Division, Indian Head

New Jersey
Galaxy, Egg Harbor

Picatinny Arsenal

Ohio
Battelle Memorial Institute, Columbus

Tennessee
British Aerospace Engineering Systems, Ordnance Systems Inc., Kingsport

Virginia
Galaxy Scientific, Blacksburg

Israel
Israel Security Agency

Ministry of Defense

United Kingdom
Defence Science and Technology Laboratories

Police Scientific Development Branch

Improvised Device Defeat

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements to more safely and effectively render terrorist improvised devices safe. Particular emphasis is placed on technologies that safely diagnose and defeat terrorist improvised terrorist devices , including large vehicle bombs (LVBs).

The Improvised Device Defeat (IDD) Subgroup develops prototype hardware and advanced techniques to render safe terrorist improvised devices as well as information and training systems for conducting threat assessments of terrorist improvised explosive devices (IEDs) and large vehicle bombs. These systems enhance the operational capabilities of the bomb disposal communities. The IDD subgroup is co-chaired by representatives from the Bureau of Alcohol, Tobacco and Firearms (ATF) and the Federal Bureau of Investigation's (FBI) Bomb Data Center.

Focus Areas

The IDD Subgroup focus areas reflect the joint priorities of military and civilian responders. During FY 2002, the IDD Subgroup focused on the following areas:

Diagnostics
Develop advanced technologies to determine the content and configuration of terrorist devices. Provide a rapid diagnostic capability for large target area coverage associated with LVBs. Focus is placed on the areas of: remote and non-intrusive identification of explosive compounds in LVBs; operational evaluation of neutron interrogation technology; and non-intrusive detection of anti-handling devices associated with IEDs.

Defeat
Develop technologies to defeat and/or render safe improvised explosive devices safely and effectively. Defeat will expand the necessary technologies to enhance the capabilities of bomb technicians to render safe improvised threat devices in large vehicle bombs.

EOD Operational Tools
Develop enhanced command and control tools, data management, and other critical incident technologies that will increase the safety and effectiveness of the EOD and bomb disposal communities. Responding to an IED incident requires detailed coordination and planning by the bomb technician's On-Scene Commander or Officer In Charge. Operational plans with standard, but flexible, operating procedures must be put into effect in order to coordinate proper equipment and personnel.

Membership

- Columbus Fire Department, Bomb Squad
- D.C. Metropolitan Police Department, Bomb Squad
- Fairfax County Police Department, Bomb Squad
- Intelligence Community
- Maricopa County Sheriffs Office, Bomb Squad
- National Bomb Squad Commanders Advisory Board
- Prince George's County Fire Department, Bomb Squad
- U.S. Capitol Police
- U.S. Department of Defense
  ACC, AFRL, DIA, Joint Services EOD, NAVEODTECHDIV, NCIS, NSA
- U.S. Department of Justice
  FBI-BDC, NIJ
- U.S. Department of Transportation
  TSA
- U.S. Department of Treasury
  ATF, USCS, USSS
- U.S. Postal Inspection Service

Remote Controlled Vehicles and Tools

Develop technologies that improve the performance and reliability of robotic systems for the bomb squad technician. These technologies include advanced robotic platforms with improved manipulation capabilities, control systems, navigation technologies, payloads, and communications. With the increasing diversity and complexity of the terrorist threat, it is vital that the bomb technician operate remotely.

Emerging Explosive Threats

Develop tools, equipment and procedures for bomb technicians to safely and effectively defeat improvised devices built from improvised materials to include non-ideal explosives. Analysis of the materials and mixtures that are emerging from threat devices will determine their performance characteristics and provide a better solution for detection and defeat of these devices.

Selected Completed Projects

Vanguard Evaluation

The commercially available Vanguard™ Robot was evaluated against NIJ requirements and met 85 percent of the critical performance parameters. Several systems have been provided to military and civilian bomb squads for evaluation.

Radio Frequency Remote Firing Device

A field evaluation of the Radio Frequency Remote Firing Device was completed using conventional explosive ordnance and IED render safe operations, range clearance operations and conventional ordnance disposal operations. During the evaluation, 30 test events were conducted using a variety of EOD tools and tactics under seven separate operational scenarios. The system met or exceeded all operational, maintenance and training requirements for EOD use, and is now available for civilian and military bomb squad communities.

Flat Panel X-Ray Evaluation

A final production unit of the portable Flat Panel X-Ray imager was completed. The existing x-ray imager was too large to meet bomb squad requirements especially in confined spaces. The thin digital imager provides a digital signal to display on a computer screen and allows it to be used when tighter physical constraints exist. The Flat Panel imager was deployed for field evaluation with selected users.

Selected Current Projects

Critical Incident Response Technology Seminars (CIRTS)

A program is being developed to bring subject matter experts directly to the bomb squads and EOD units at regional seminars in the United States. These seminars will provide briefings on critical incident response technology, use of new tools in hands-on exercises and demonstrations, and provide direct feedback from the EOD/bomb squad user.

Smart Shirt

The Smart shirt will incorporate plug and play sensors for monitoring the vital signs of First Responders. Instrumentation will monitor heart and respiration rate, electro-cardiogram, and body temperature. Voice and data communication are also planned for integration. The user's vital signs will be transmitted, wirelessly, to a monitoring station. The monitoring station will provide feedback to the individual and incident commander.

PELAN Commercialization

A portable non-intrusive diagnostic system that is capable of identifying explosives or other hazardous ingredients of improvised explosive devices is being developed. The system differentiates between explosives and innocuous materials in a non-intrusive non-destructive manner. The substances are identified by the characteristic gamma rays emitted from the object during neutron irradiation. Two prototype units will be built and deployed for advanced operational test and evaluation.

Recoilless Disruptor

A disrupter mounting system is being developed to reduce the risk of damage to the robot from recoil. The recoilless mitigation system will be capable of adapting to any of the disruptors in use by Federal, State, and Local Bomb Squads.

Next Generation EOD Remote Control Vehicle

Technology for the next generation of Robotic vehicles is being developed for EOD applications. The developed technology will focus on the following areas: wheeled platforms capable of climbing steep grades and stairs, traversing water, and operating in the most rugged and challenging environments; a "light," tracked platform with a small footprint and extremely high mobility; a dextrous manipulator capable of lifting heavy loads and withstanding disrupter recoil forces; and multiple communication mediums.

Contact Information

iddsubgroup@twsg.gov

Performers

California
Science Applications International Corporation (SAIC), San Diego

Colorado
Applied Research Associates, Littleton

District of Columbia
U.S. Naval Research Laboratory

Florida
Air Force Research Lab, Tyndall AFB

Indiana
Golden Engineering, Centerville

Kentucky
Western Kentucky University, Bowling Green

Maryland
Naval Explosive Ordnance Disposal Technology Division, Indian Head

Massachusetts
iRobot, Somerville

Nevada
Sparta, Inc., Las Vegas

New Mexico
Applied Research Associates, Albuquerque
Sandia National Laboratories, Albuquerque

New York
Sensatex, New York

Ohio
Battelle Memorial Institute, Columbus

Oklahoma
Nomadics, Stillwater

Pennsylvania
Franklin Applied Physics, Oaks

Rhode Island
University of Rhode Island, Kingston

Tennessee
Northrop Grumman, REMOTEC, Oak Ridge

Texas
Applied Research Associates, San Antonio

Virginia
Booz•Allen & Hamilton, McLean

Canada
EOD Performance, Ontario
MREL, Ontario

United Kingdom
Defence Science and Technology Laboratories

Infrastructure Protection

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for the protection and assurance of critical Government, public, and private infrastructure systems required to maintain the national and economic security of the United States.

The Infrastructure Protection (IP) Subgroup works to ensure the uninterrupted service of the infrastructure systems that are vital to maintaining the national and economic security of the United States. These critical systems include control systems for electric power, natural gas, petroleum products, and water; telephone, radio, and television communications systems; ground, rail, and air transportation facilities; and cyber communications networks. The IP Subgroup R&D reflects the multivariate threat to the complex and interdependent systems, subsystems, and components of the nation's infrastructure. Solutions include conventional security measures as well as those offered by emerging technologies. Representatives from the Department of Defense and the FBI National Infrastructure Protection Center (NIPC) chair the subgroup.

Focus Areas

The IP Subgroup focus areas reflect the prioritized requirements generated with respect to the critical aspects of the nation's infrastructure. During FY 2002, the TSWG IP Subgroup focused on the following areas:

Physical Protection

Develop standardized methodologies and decision aids for vulnerability analysis and enhanced protection of elements critical to the nation's infrastructure. These critical elements include power generation and transmission systems, water supplies, and health services. After understanding the dynamics of complex critical infrastructures, secure operating methodologies and strategies can be developed to prevent or mitigate widespread failures due to cascading and interactive network effects. Hidden interdependencies are likely causes for failure because complex linkages and infrastructure dependencies are poorly documented. Dynamic behavior models of cascading effects will be evaluated; common standards and practices within and between critical infrastructures will be developed, and system vulnerabilities to various weapons will be investigated.

Cyber Security

Develop detection, prevention, response, and alert capabilities to strengthen electronic information and control systems and to counter cyber-attacks. Prevention and mitigation of threats to computer networks is vital to Homeland Security since society increasingly relies

Membership

- Environmental Protection Agency
- Federal Emergency Management Agency
- Nuclear Regulatory Commission
- U.S. Department of Agriculture
  FS
- U.S. Department of Commerce
  CIAO, NIST
- U.S. Department of Defense
  AFOSI, DTRA, JFCOM, JPO-STC, NCIS, NSWC, USACE
- U.S. Department of Energy
- U.S. Department of Justice
  FBI, NIPC
- U.S. Department of the Treasury
  USSS
- U.S. Department of Transportation
  FAA

upon new information technologies and the Internet to conduct business, manage industrial activities, engage in personal communications, and perform scientific research. The complexity of information technologies and their widespread integration increase the likelihood of unforeseen vulnerabilities. Unprecedented opportunities to steal money or proprietary data, invade private records, conduct industrial espionage, or cause vital infrastructure failures are available to terrorists, criminals, and hostile nations through the global reach of the Internet.

Selected Completed Projects

Water Flow Modeling

Software applications were developed to model the transport and dispersion of biological and chemical contaminants in both natural and manmade water distribution systems in regions of the United States. The Real Time River Spill System (RiverSpill) and the Pipeline Network Modeling System (PipelineNet) are the models delivered to analyze the contaminant propagation. These models are used to determine the extent of contamination and the area and population that will be affected. These models were used and played an integral role in the security planning and preparation for the Olympics in Salt Lake City. Work continues to provide greater national coverage.

Selected Current Projects

Systems Administrator Simulation Trainer

The Systems Administrator Simulation Trainer (SAST) is being created as an experience-based, distance-learning environment for computer system administrators to learn how to apply a broad range of host and network-based security tools and techniques. SAST will test the ability of trainees to defend against a diverse cyber threat environment by applying a variety of cyber offensive tools. SAST will efficiently provide system administrators with real world experience in resisting, responding to, and recovering from cyber attacks.

Automated Risk Assessment Methodology For Dams

The Risk Assessment Methodology for Dams (RAM-D) is a standardized approach to risk assessment and draws on existing techniques and practices tuned specifically to the needs of dams and dam operators. Following the successful development and validation of the basic RAM-D field manual, this task will automate the methodology in order to simplify its use and increase its value to a larger community. Future efforts are planned to expand the existing capabilities to include bridges, tunnels, and transmission lines.

Supervisory Control and Data Acquisition Protection II

A prototype cryptographic module is being developed and will include a suite of algorithms to meet the needs of Supervisory Control and Data Acquisition (SCADA) users. The cryptographic module's ability to safeguard transmissions between master and remote terminal units and to deny unauthorized data transmissions or intrusions will be tested and evaluated. The software/hardware configuration is being designed to be acceptable to both users and

manufacturers, economically feasible, and suitable for installation in new and existing systems.

Alert Trend Change Detection For Network Intrusions

The Alert Trend Change Tool (ATrCT) is a tool that will improve analysts' understanding of the numbers of hostile alerts and scans detected on a given computer network.. ATrCT uses an algorithm to analyze data collected by both freeware and custom software sensors to help protect a network against malicious autonomous agents. It provides analysts with warning indicators when sensors detect increased scanning activity against a particular service or an increase in the frequency of a particular alert. This will help analysts detect hostile activity sooner, and therefore react more quickly to a new threat. The second Code Red outbreak in August 2001, for example, was characterized by a near doubling of the number of attacking machines each hour in the early hours of the outbreak. ATrCT would detect and report this type of behavior to analysts, who could in turn react quickly to prevent infection or repair infected machines.

Communications Firewall

A proof of concept Communications Firewall system that ensures communication security by actively monitoring all telecommunications traffic entering and leaving secure facilities is being developed. The system is currently built for a Nortel CTS switch, and provides a capability for any anomaly to be reported via secure connection to a control center responsible for facility security. The Communications Firewall system monitors alarm circuits, analog and digital phones, trunked lines (fiber and metallic), STU-III, fax (secure and non-secure) and modems. Future work may include LAN/WAN, T-1/E-1 circuits, video, cable TV, classified circuits, and other circuits installed in the facility. The system allows for remote programming, remote software upgrades, and monitoring of active circuits.

Contact Information

ipsubgroup@tswg.gov

Performers

California
Applied Signals Technology, Sunnyvale

Illinois
Gas Technology Institute, Des Plaines

Massachusetts
Massachusetts Institute of Technology, Lincoln Laboratory, Lexington

Virginia
Booz·Allen & Hamilton, McLean

Naval Surface Warfare Center, Dahlgren

Science Applications International Corporation (SAIC), McLean

SRA International Inc., Fairfax

Washington
Pacific Northwest National Laboratory, Richland

Investigative Support and Forensics

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements for criminal investigation, law enforcement, and forensic technology applications in terrorism-related cases.

The Investigative Support and Forensics (IS&F) Subgroup supports research and development projects intended to provide new capabilities to law enforcement personnel, forensic scientists and intelligence operatives responsible for investigating and interdicting terrorist incidents. Work conducted under the auspices of this group has had a major impact on forensic investigations and intelligence operations throughout the world of law enforcement. Representatives from the U.S. Secret Service (USSS) and U.S. Postal Service (USPS) chair the subgroup.

Focus Areas

The IS&F Subgroup focus areas reflect the prioritized requirements of the military and civilian law enforcement communities. During FY 2002, the TSWG IS&F Subgroup focused on the following areas:

Digital Evidence Examination
Develop "next generation" technologies to improve the recovery and analysis of digital evidence (computer media, wireless data, and digital audio or video imagery). A computer forensics examination system with specially configured hardware and software is being developed to access computer drives, catalog the files, and identify known program executables, data files, and system software without alerting the suspects. In addition, software tools used to examine electronic evidence are being validated and their capabilities and limitations are being verified. The results of this validation will be recorded in a nationally accessible database. Finally, the investigative capabilities associated with pervasive computing, such as the linking of computer processors, networks, and data repositories with "smart" devices (e.g., personal digital assistants, cell phones with wireless data modems) are being improved.

Energetic and Hazardous Materials Examination
Develop advanced technologies pertaining to crime scene response, explosive and arson debris examination, transfer (trace) evidence, as well as three-dimensional digital photographic modeling and laser photogrammetry of crime scenes.

Forensic Biology and Molecular Biochemistry
Develop techniques for recovering and analyzing DNA on material and surfaces to support forensic investigations and intelligence

Membership

- Environmental Protection Agency
- Federal Emergency Management Agency
- Intelligence Community
- National Forensic Science Technology Center
- U.S. Department of Commerce
  NIST-OLES
- U.S. Department of Defense
  AFIP, CBIRF, CIDC, DTRA, DoDPI, FPSPO, NCIS, NSA
- U.S. Department of Justice
  DEA, FBI, NCFS, NIJ, USMS
- U.S. Department of Transportation
  TSA
- U.S. Department of Treasury
  ATF, IRS, USCS, USSS
- U.S. Postal Inspection Service
- U.S. Postal Service

operations. Within this area, techniques for the rapid analysis of stable isotope ratios at natural abundance levels for forensic applications are being developed.

Friction Ridge Analysis

Optimize friction ridge analysis and fingerprint recovery methods. Less expensive and more robust, sensitive, and environmentally safe physical developers and visualization techniques are being created. In addition, new technologies for recovering DNA from fingerprints are being produced and the genetic basis and statistical significance of specific print features are being determined. The forensic defensibility of latent print evidence is being strengthened through the employment of digital imaging technologies. Finally, the chemical content of latent prints is being characterized.

Questioned Document Examination

Investigate the uniqueness of and variation within an individual's handwriting through scientific analysis. An automated system for forensic examination and identification of suspect handwriting and documents is also being developed.

Surveillance Technology

Develop advanced technologies for invisibly marking moving or stationary targets that may be imaged remotely, day or night. Special application beacons, advanced optical lenses, and special application chemical tags are being developed as well.

Selected Completed Projects

Computer-Based First Responder's Planning and Decision Tool

The initial actions taken at chemical or biological incidents significantly impact the outcome. This real-time computer-based first responder's planning and decision tool, commercially produced as the "Chemical/Biological Response Aide" or CoBRA™, was designed to provide first responders with a planning and rapid decision support tool. CoBRA™ assists first responders in determining the severity and nature of a threat, and in identifying, dispatching, and controlling emergency resources. It has been fielded with federal, state, and local first responders.

Chemical Development of Latent Fingerprints

The ability to recover and visualize identifiable latent fingerprints from some surfaces has been challenging to investigators. This capability was recently enhanced through the development of 1,2-indanedione, a new fingerprints reagent. Conducted under a bilateral agreement with Israel, a more sensitive process for developing latent fingerprints on paper was developed. The process, published in forensic science journals, has proven valuable in identifying assassins.

Selected Current Projects

Authentication of Digital Video Images

A handheld audio-video camcorder with an anti-spoofing digital recording format that establishes a means to authenticate the digital video original recording from any subsequent copies is being developed. The equipment will ensure that original recordings cannot be altered, manipulated, or edited to ensure admissibility in court proceedings. The camcorder will also be capable of extremely low light recording.

DNA Recovery from Processed Fingerprints

Forensic researchers are developing improved techniques for extracting and identifying DNA from partial, chemically developed prints insufficient for identification. To obtain sufficient visualization, partial prints are subjected to severe chemical conditions and may contain minimally testable amounts of DNA. In response to these matters, protocols for short tandem repeat DNA, mitochondrial DNA, and Alul DNA, conforming to guidelines required for search and identification within the national DNA (CODIS) database, are being optimized.

Computer Forensics Processing Suite

A "next generation" computer forensics software examination tool for multiple platforms is being developed. The tool will add capabilities, such as emulation drivers and pattern analysis tools for redundant array of independent disks (RAID).

Fingerprint Optimization

The interaction of paper, deposited latent prints, environmental conditions, and print developing reagents are being examined in order to optimize fingerprint development procedures.

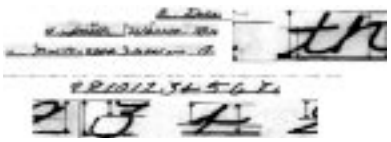
Hyperspectral Imager for Document Examination

Hyperspectral imagers are being enhanced to exploit their potential for document examination and other forensic hyperspectral imaging applications. More specifically, a high spatial and spectral resolution bench top hyperspectral workstation with extended UV and Near-IR capability is being developed to improve the forensic capability of document examination.

Link Analysis of Computers Through Reachback Signals

Equipment that links computer diskettes and other data to an individual disk drive and computer by the modulation signals within the hardware is being developed. The equipment will forensically link a computer to an attempted or actual penetration of a U.S. government computer network. The identification of individual characteristics of a computer or computer storage media by the associated modulation signals and the link between questioned and known data objects is also being explored.

Handwriting Comparison of Different Character Sets



The forensic capability to compare a questioned document written in one language (and associated character sets), such as Cyrillic or Arabic, with known handwriting samples in a different language (character set), such as English, is being developed. Preliminary analysis has determined that there are similarities in letter design, initial strokes, touching of letters, spacing, and connections. The resulting method/technique will be subjected to peer review and scientific validation. The final procedure will conform to case law and evidentiary standards.

Contact Information

isfsubgroup@tswg.gov

Performers

California
3rd Ring, Mammoth Lakes

Florida
Florida International University, Miami
University of Florida, Gainesville

Maryland
Johns Hopkins University Applied Physics Laboratory, Laurel
National Institute of Technology, Gaithersburg

Massachusetts
Massachusetts Institute of Technology (MIT), Lincoln Laboratory, Lexington

Minnesota
Honeywell Laboratories, Minneapolis

Mississippi
ProVision Technologies, Stennis Space Center

North Carolina
Signalscape, Raleigh

Ohio
Ohio University, Clippinger Labs, Athens

Pennsylvania
Carnegie Mellon University, Pittsburgh

Texas
BAE Systems, Austin

Virginia
The Bode Technology Group, Springfield
Veridian Information Systems, Inc., Arlington

Washington
Pacific Northwest National Laboratory, Richland

Australia
Queensland University of Technology, Brisbane

United Kingdom
Forensic Science Service
Police Scientific Development Branch

Personnel Protection

Mission

Develop unique equipment and systems to prevent and mitigate attacks on VIP protectees. This includes hardware and tools that provide security to both the VIPs and their protectors. Inherent in this development is additional emphasis on life safety and emergency response equipment.

The Personnel Protection (PP) Subgroup develops protection equipment, diagnostic and reference tools and standards that support greater security for VIPs. In order to be effective, personnel who are charged with the safety of these VIPs must also have protective equipment that will prevent injury and tools that will improve their effectiveness. These developments increase the operational effectiveness of federal, state, military, and local law enforcement personnel who are charged with the protection of VIPs. These technologies and tools also have application to the protection of military and law enforcement personnel who engage in hazardous combat-like environments. A representative from the U.S. Secret Service chairs the subgroup.

Focus Areas

The PP Subgroup focus areas reflect the prioritized requirements of the VIP protection community. During FY 2002, the TSWG PP Subgroup focused on the following areas:

Vehicle Protection and Performance
Develop technologies related to the performance, security, integrity, and armoring of fully-armored passenger vehicles, especially those that increase the safety of passengers during sniper or blast attacks.

Transparent Armor Development
Develop advanced light weight transparent armor that will provide improved protection over existing technology.

Individual Protection Systems
Develop improved body armor and standards to provide greater effectiveness against current and emerging threats.

Counter Sniper Measures
Develop and evaluate technologies that will provide protective details with indications and warnings of, and protection from sniper and remote attacks.

VIP Installation Protection
Develop systems to enhance the protection of critical installations with early warning and alerting for protective teams.

Membership

U.S. Department of Commerce
NIST-OLES

U.S. Department of Defense
Natick RD&E Center, TACOM

U.S. Department of Energy
OS

U.S. Department of Justice
NIJ

U.S. Department of Labor
OIG

U.S. Department of State
DS

U.S. Department of the Treasury
USSS-SSD, USSS-TSD

Selected Completed Projects

Hybrid Composite Armor

The use of alternative materials for armoring vehicles has the potential to greatly improve the efficiency of installation and to reduce the overall weight of the vehicle, while maintaining or improving ballistic protection. This type of armor can be easily integrated into the vehicle, thereby saving cost and improving overall effectiveness of the armor. This project evaluated a buildup of carbon fiber and spectra shield material in a matrix. This material can be combined with other ceramic materials to increase the protection against rifle threats. The developments from this program have had direct application for use in rifle-rated (NIJ Level IV) body armor as small arms personnel insert plates.

Selected Current Projects

Armored Passenger Vehicle Standards

There currently exists no U.S. standard describing the performance of non-tactical armored passenger vehicles (APVs). Protocols will be developed to evaluate a full range of armored passenger vehicles to meet the user requirements. These standards will be applicable to all APVs designed to provide protection in noncombat situations. Five critical areas will be addressed: ballistic resistance, blast resistance, automotive performance, transparent armor optical quality, and quality control. This effort will provide a graduated set of standards for a given level of protection.

Body Armor Aging and Environmental Effects

The impact of aging and environmental effects on the performance and reliability of body armor is being evaluated to determine if there are significant factors that may result in sub-standard performance. This testing will likely be used to evaluate the proper care of body armor and eventually will lead to the development of criteria for removing armor from use prior to its scheduled warranty or planned retirement.

Female Body Armor Assessment

Unique construction of female body armor will be evaluated to develop a better understanding of those effects that could result in more significant injuries to the wearers. The results of these studies will be coordinated with the existing NIJ standards for personnel body armor.

Body Armor Cooling System

Wearing body armor in hot climates, particularly for long periods, is physiologically stressful and can compromise the wearers' efficiency. In some cases the wearer may be inclined to remove the armor. An under armor cooling system has been developed and found to be effective. Recommendations provided by users in operational scenarios are being incorporated into an upgrade of the cooling system's design. The resultant system will be lightweight and will provide comfort to wearers. It is expected to provide cooling for up to several hours without having to replace the cooling media.

Testing Methodology for Ballistic Helmets

New standardized protocols will be developed to establish performance of ballistic helmets. These protocols will be published as a set of standards that will be endorsed by the National Institute for Standards and Technology.

Sniper Detection and Warning

The ability to identify a potential sniper before the first shot is a high priority requirement for VIP protection. A system that will locate potential sniper activity is being developed. Potential threats will be identified and their positions marked to allow protection detail personnel to respond promptly.

Contact Information

ppsubgroup@tswg.gov

Performers

Alabama
Missile and Space Intelligence Center, Huntsville

Arkansas
Tekne Group, Inc., Hot Springs

California
ACM Systems, Rancho Cordova

SPAWAR Systems Center, San Diego

Georgia
Georgia Tech Research Institute, Smyrna

Idaho
Idaho National Engineering and Environmental Laboratory, Idaho Falls

Massachusetts
Surmet, Burlington

Technical Products, Inc., Wayland

Michigan
Triad Services Group, Madison Heights

Wayne State University Bioengineering Center, Detroit

New Mexico
Science and Engineering Associates, Inc., Albuquerque

Nevada
Bechtel–Remote Sensing Laboratory, Las Vegas

Ohio
University of Dayton Research Institute, Dayton

Texas
Applied Research Associates, San Antonio

Northrop Grumman-Litton Electro Optical Systems, Dallas

Southwest Research Institute, San Antonio

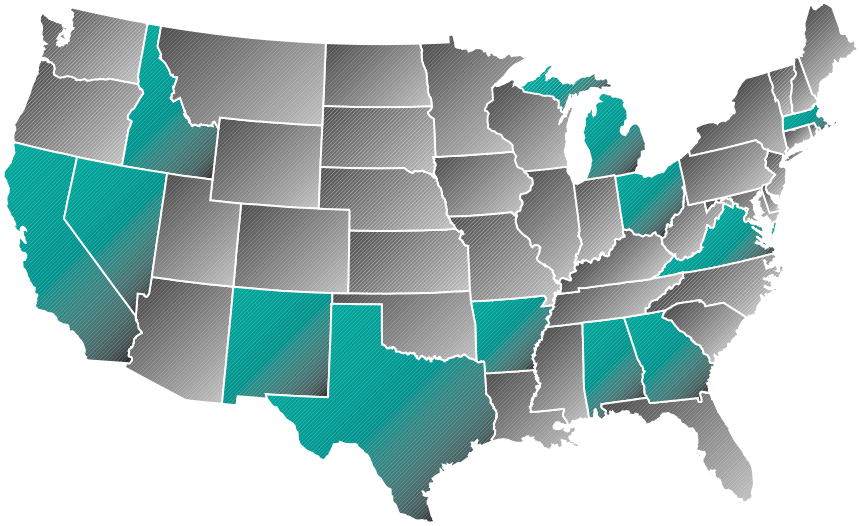
Virginia
General Testing Laboratories, Colonial Beach

QinetiQ, Arlington

Israel
Israel Security Agency

Israeli National Police

Ministry of Defense



Physical Security

Mission

Identify and execute research and development projects that satisfy interagency requirements for physical security support to protect personnel, equipment and facilities against terrorist attack.

The Physical Security (PS) Subgroup identifies the physical security requirements of federal agencies, both within the United States and abroad, and develops the technology to protect their personnel and property from terrorist attack. The subgroup develops this technology by creating prototype hardware, software, or systems for technical and operational evaluation by user agencies. A representative from the DoD chairs the subgroup.

Focus Areas

The PS Subgroup focus areas reflect the prioritized requirements of the physical protection community. During FY 2002, the TSWG PS Subgroup focused on the following areas:

Blast Mitigation
Develop building construction and retrofit techniques that better protect people and facilities from the two main causes of injuries resulting from terrorist bomb blasts – flying debris and structural collapse.

Entry Point Screening
Develop multiple technologies and techniques to detect explosives, weapons, chemical and radiological material, and other contraband on or in personnel, vehicles, vessels, cargo, and mail. Solutions will increase the detection rate, throughput, and safety while reducing the number of security forces required to perform the screening process.

Perimeter Protection
Develop advanced perimeter intrusion detection and surveillance systems that have a higher probability of detection, a lower false alarm rate, and the ability to operate continuously in demanding operational environments. These systems will provide security forces with improved early warning and response capabilities on land and at sea.

Selected Completed Projects

Military Mobile Vehicle and Cargo Inspection System (MMVACIS)
MMVACIS, a mobile gamma radiation imaging system, was developed for the inspection of vehicles and cargo. The system provides rapid deployment capability to established bases or with U.S. expeditionary forces. It has been employed by a DoD Command since fall 2001, and has been integrated into contraband interdiction and force protection operations.

Membership

- Federal Emergency Management Agency
- General Services Administration
  FPS
- Intelligence Community
- Nuclear Regulatory Commission
- Supreme Court of the United States
- U.S. Department of Defense
  CENTCOM, DIA, DLA, DTRA, EUCOM, JCS, JFCOM, NRO, NSA, OASD (C3I), OUSD (AT&L), PACOM, PFPA, USA, USAF, USMC, USN
- U.S. Department of Energy
  NNSA, OS
- U.S. Department of Justice
  FBOP, NIJ
- U.S. Department of State
  DS
- U.S. Department of the Treasury
  ATF, FRB, USCS, USSS
- U.S. Department of Transportation
  OIS, TSA, USCG
- U.S. Postal Service

Quick Reaction Perimeter Intrusion Detection Sensor (QUPID)

QUPID is an ultra-wide-band impulse radar system with adjustable range gates that projects a "virtual fence" beyond the perimeter to detect intruders at distances up to 100 meters. TSWG successfully developed two prototype versions of the sensor in FY 2002: the first is compatible with the USAF Tactical Automated Security System and the second works with a commercial intrusion detection system. The Air Force transitioned QUPID into an acquisition program in July 2002 with fielding planned for FY 2003.

High Volume Mail Room Scanner

A portable high-volume mail scanner was developed to rapidly scan and segregate parcels and flat mail that may contain improvised explosive devices. Two prototype systems were produced. One was deployed for security operations at the 2002 Olympics in Salt Lake City and the other is at a U.S. military postal center in Germany.

Composite Retrofit Methods

Retrofit design concepts and guidelines for strengthening existing reinforced concrete buildings against terrorist bomb attacks were developed. Composite retrofit techniques, such as spray-on polymers and column wraps have been evaluated and design guidance written. These techniques have been used to upgrade embassies and military facilities.

Vessel Identification and Positioning System (VIPS)

VIPS uses differential GPS-based (DGPS) transponders and shore-side base stations to track maritime security forces in high threat ports. VIPS also tracks host nation support watercraft. The system includes several tamper awareness systems. In July 2002, VIPS was integrated into an East Coast port security operation.

Selected Current Projects

Early Warning and Detection of Adversary Intrusions

A critical need exists for early detection of intruders at long-range outside installation perimeters. A portable, long-range surveillance system capable of automatically detecting individuals and vehicles at ranges up to 4 kilometers, day or night, is being developed. The system is designed for either fixed operation at established bases or rapid deployment with U.S. expeditionary forces. The prototype system consists of a forward looking infrared (FLIR) video camera with optical zoom for night detection, a daytime video camera with optical zoom, a laser range finder, and an operator monitor. During FY 2003, the prototype system will be operationally evaluated.

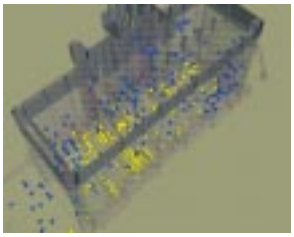
Lightweight Portable Boom and Underwater Sentry System

A lightweight boom, equipped with fiber optic and acoustic sensors to provide standoff detection of intruders for U.S. Navy ships, is being developed. It is designed for easy deployment and redeployment by the ship's crew dockside or at anchor in transit ports. It will provide a temporary legal perimeter barrier as well as surface and subsurface intrusion detection capabilities against attacks by small boats and swimmers. The prototype system will continue developmental testing and evaluation during FY 2003, and will begin operational testing in FY 2004.

Ground Surveillance Radar for Perimeter Intrusion Detection

Existing Airport Surface Detection Equipment (ASDE-3) ground surveillance radar, used at U.S. airports to track aircraft and vehicles on the ground, is being adapted to improve airport perimeter security. An Airport Security Display Processor (ASDP) is being developed to display ground surveillance radar and existing perimeter intrusion detection systems data on one central processing station. The ASDP's combined real-time data will provide airport security forces with a better capability for detecting perimeter intrusions. A prototype ASDP will be tested at a U.S. airport in FY 2003.

Blast Effects Estimation Model (BEEM)



BEEM will be a single model capable of estimating the effects of blasts, fragmentation, building damage and personal injury. BEEM will incorporate the best features of two existing models, the Force Protection Tool (FPT) and the Anti-Terrorism Planner (AT-Planner) tool.

Glass Penetration Model

A human injury prediction model based on multi-hit glass penetration is being developed. The model inputs will be window characteristics, blast parameters, and the location of a person relative to the window. The model will output the severity of the injuries to that person. The final product will be a software model that will complement BEEM.

Advanced Vehicle Driver Identification System

The Advanced Vehicle Driver Identification System (AVIDS) is being developed to expedite the screening process at vehicle entry points by providing force protection personnel with near real-time access to control databases. This modular system allows users to select only those components needed at their facility. AVIDS has been installed at a DoD facility, enabling verification of the occupants of a vehicle in less than three seconds over a secure wire-less LAN that covers eighteen square miles and five vehicle entry points. Weigh-in-motion, RF tags, and license plate reader modules will be integrated by the end of 2002, with biometrics modules integrated in 2003.

Performers

Arizona
Thunder Mountain Evaluation Center, Sierra Vista

California
Karagozian & Case, Glendale
Naval Facilities Engineering Command, Port Hueneme
Petrogen, San Leandro
Science Applications International Corporation (SAIC), San Diego
SRI International, Menlo Park

Florida
ANRO Engineering, Inc., Sarasota
Megaseal Corporation, Miami
U.S. Air Force Civil Engineering Support Agency, Tyndall AFB
U.S. Air Force Force Research Laboratory, Tyndall AFB

Indiana
Creative Building Products, Inc., Fort Wayne

Maryland
Atlantic Coast Technologies, Silver Spring
Technology Service Corporation, Silver Spring

Massachusetts
Curtiss Wright/Lau Defense Systems, Inc., Littleton
U.S. Air Force Electronics Systems Center, Force Protection C2 Systems Program Office, Hanscom Air Force Base
Volpe National Transportation Systems Center, Cambridge

Mississippi
U.S. Army Corps of Engineers, Engineering Research and Development Center, Waterways Experimental Station, Vicksburg

Nebraska
U.S. Army Corps of Engineers, Protective Design Center, Omaha
University of Nebraska, Lincoln

New Mexico
Applied Research Associates, Albuquerque
New Mexico Tech Energetic Materials Research & Testing Center (EMRTC), Socorro
Sandia National Laboratories, Albuquerque

New York
Ocean & Atmospheric Science, Dobbs Ferry
Weidlinger Associates, Inc., New York

Ohio
Battelle Memorial Institute, Columbus

Tennessee
PIPS Technology, Knoxville

Texas
EQE International, San Antonio
U.S. Air Force Force Protection Battlelab, San Antonio
U.S. Army Institute of Surgical Research, San Antonio
Wilfred Baker Engineering, Inc., San Antonio

Virginia
Defense Threat Reduction Agency, Alexandria
Naval Surface Warfare Center, Dahlgren Division
Science Applications International Corporation (SAIC), McLean
Tetratech, Inc., Falls Church
U. S. Army Night Vision & Electronic Sensors Directorate, Ft. Belvoir
U.S. Army Product Manager for Physical Security Equipment, Ft. Belvoir
U.S. Army Software Engineering Center, Ft. Belvoir

Washington
Pacific Northwest National Laboratories, Richland

Israel
Israel Security Agency
Ministry of Defense

United Kingdom
Defence Science and Technology Laboratories

Surveillance, Collection and Operations Support

Mission

Identify, prioritize, and execute research and development projects that satisfy interagency requirements supporting intelligence gathering and special operations directed against terrorist activities.

The Surveillance, Collection and Operations Support (SC&OS) Subgroup identifies high-priority user requirements and special technology initiatives focused primarily on countering terrorism and offensive operations. The research and development projects supported by the subgroup reduce the capabilities and support available to terrorists and enhance U.S. capabilities to conduct retaliatory or preemptive operations. A representative from the Intelligence Community chairs the subgroup.

Focus Areas

The SC&OS Subgroup focus areas reflect the prioritized requirements of the Intelligence Community. During FY 2002, the TSWG SC&OS Subgroup focused on the following areas:

Traditional Surveillance
Improve capabilities for the covert collection and enhancement of video, imagery, and audio surveillance, considering that success in countering terrorism often depends on the quality of intelligence collection.

Analytic Surveillance
Improve the means for detecting terrorists by developing automated tools that utilize biometrics, pattern recognition, voice and speaker recognition, and database technologies to identify terrorists.

Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C^4ISR)
Develop programs and initiatives, such as tagging, tracking and locating (TTL), special sensors, and covert communications, that improve the capability to locate, identify, and track terrorists and terrorist activities.

Information Operations (IO)
Exploit digital information age technology through the development and optimization of tools used to degrade, disrupt, deny or destroy adversary information and information systems.

Program

SC&OS programs are classified or sensitive. Program requirements or the success of programs and specific program capabilities cannot be discussed in an open document.

Membership

Intelligence Community

U.S. Department of Defense
DIA/CMO, NRO, NSA, SOCOM

U.S. Department of Justice
DEA, FBI

U.S. Department of the Treasury
USCS, USSS

Contact Information

scossubgroup@tswg.gov

Performers

Arizona
Authenti-Corp, Gilbert

California
San Jose State University, San Jose

Special Technologies Laboratory, Santa Barbara

Virage Inc., San Mateo

Florida
Harris Government Communications Systems Division, Melbourne

Maryland
Eumetria Inc., Columbia

Massachusetts
BBN Technologies, Cambridge

Viisage Technology, Littleton

New Jersey
Sarnoff Corporation, Princeton

New Mexico
Sandia National Laboratories, Albuquerque

Virginia
Applied Marine Technology Incorporated, Virginia Beach

Autometric Incorporated, Springfield

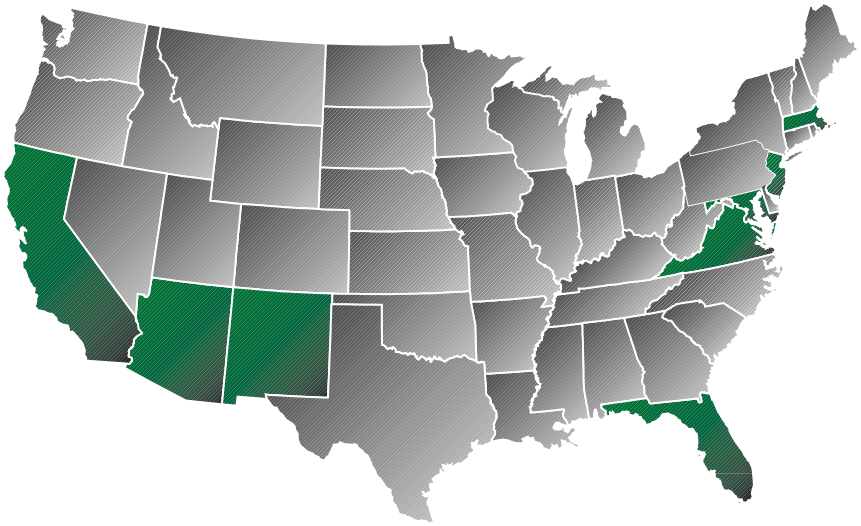
ORION Scientific Systems, McLean

Canada
Defence Research Establishment, Suffield

Israel
Ministry of Defense

United Kingdom
Defence Science and Technology Laboratories

Police Scientific Development Branch



Tactical Operations Support

Mission

Develop equipment and systems to support specialized force offensive operations directed against terrorist activities and groups; to make non-sensitive prototype hardware available for commercial production to assist military base commanders, state, and local enforcement agencies.

The Tactical Operations Support (TOS) Subgroup supports counterterrorist tactical operations, particularly those performed by specialized forces trained for assault operations. The subgroup supports technology development activities, which provide a foundation for subsequent advances, and the development of prototype special equipment designed to facilitate more effective execution of various tactical missions. The principal users of the technology developed by this subgroup are the Military Special Forces, the FBI-Hostage Rescue Team, DOE nuclear security teams, and the U.S. Secret Service. A representative from the DoD chairs the subgroup.

Focus Areas

The TOS Subgroup focus areas reflect the prioritized requirements of offensive counterterrorism forces. During FY 2002, the TSWG TOS subgroup focused on the following areas:

Advanced Imaging Systems
Develop advanced optical systems to provide improved imaging in night and obscured viewing environments.

Specialized Access Systems
Develop systems that will enhance access to tactical objectives and improve tactical efficiencies in assault operations.

Chemical and Radiation Detectors
Develop small, rugged chemical and radiation detection systems for use by specialized teams in tactical operations.

Offensive Systems
Develop unique equipment for use in special operations tactical missions.

Tactical Communications Systems
Develop unique communications systems and capabilities used in special operation environments with special considerations for assault team requirements.

Membership

U.S. Department of Defense
SOCOM

U.S. Department of Energy
OS

U.S. Department of Justice
FBI

U.S. Department of the Treasury
USSS

Program Highlights

Program and Subgroup Detail

TOS programs are classified or highly sensitive. Program requirements or the success of programs and specific program capabilities cannot be discussed in an open document.

Contact Information

tossubgroup@tswg.gov

Performers

Arizona
Armorworks, Tempe
Litton Electro-Optical Systems, Phoenix

California
Lawrence Livermore National Laboratory, Livermore
Science Applications International Corporation (SAIC), San Diego
Special Technologies Laboratory, Santa Barbara

Florida
Knights Armament Company, Vero Beach

Indiana
Naval Surface Warfare Center, Crane Division

Maryland
Multispectral Solutions, Inc., Germantown

Massachusetts
Charles Stark Draper Lab, Cambridge
MITRE, Bedford

New Hampshire
Impact Science and Technology, Hollis
Wilcox Industries, Portsmouth

New Jersey
U.S. Army Communications Electronics Command (CECOM), Ft. Monmouth

Ohio
Battelle Memorial Institute, Columbus

Pennsylvania
Optical Systems Technology, Inc., Freeport

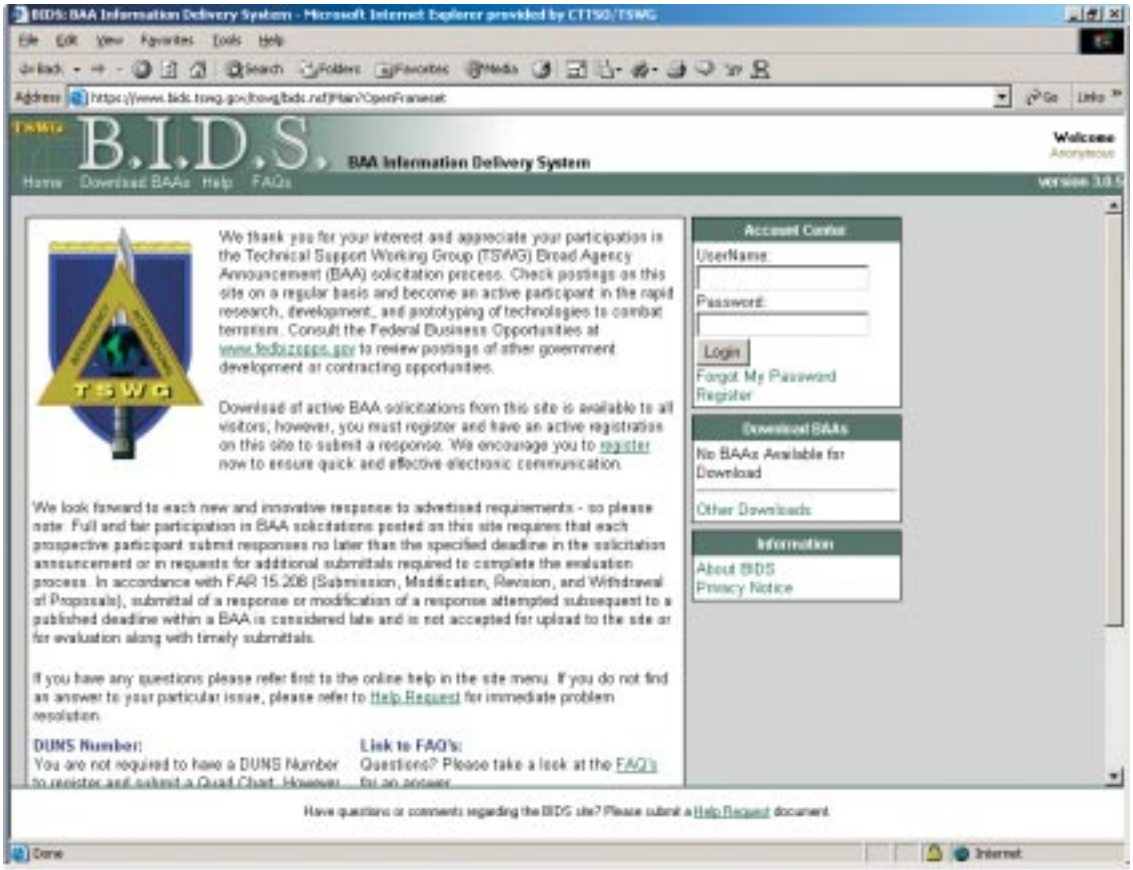
Israel
Ministry of Defense

TSWG 2002 REVIEW

APPENDICES

BAA Information Delivery System (BIDS)

TSWG seeks technology solutions that address operational and technological shortfalls identified by Government agency users at least once annually. User requirements are disclosed in a solicitation format called a Broad Agency Announcement or "BAA." The BAA enables the Government to solicit industry, academia and Government Laboratories for innovative research and development solutions to these requirements. The BAA is advertised in the Federal Business Opportunities at www.fedbizopps.gov. The FedBizOpps site will direct interested bidders to the appropriate web address where additional information for submitting a proposal is posted. Each open BAA is always posted at the TSWG program website: www.bids.tswg.gov. The application at this website is called the BAA Information Delivery System or "BIDS." BIDS provides an electronic submission and record evaluation capability for receiving and evaluating responses to BAA. BIDS is a secure 128-bit encryption that provides proposal response uploads for prospective bidders and ensures control of bidder proprietary data.



TSWG Subgroup Membership

Chemical, Biological, Radiological and Nuclear Countermeasures

Amtrak Police Department

Environmental Protection Agency

Federal Emergency Management Agency

General Services Administration
- Federal Protective Services

Intelligence Community

InterAgency Board

Nuclear Regulatory Commission

U.S. Capitol Police

U.S. Department of Agriculture
- Agricultural Research Service
- Animal and Plant Health Inspection Service
- Food Safety and Inspection Service
- Office of the Inspector General

U.S. Department of Commerce
- National Institute of Standards and Technology

U.S. Department of Defense
- Biological Chemical Joint Operations Center
- Central Command
- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Protective Service
- Defense Threat Reduction Agency
- Joint Chiefs of Staff
- National Security Agency
- Office of the Assistant to the Secretary of Defense/Chemical and Biological Defense
- Special Operations Command
- U.S. Air Force
  - Air Combat Command
  - Electronic Systems Center
  - Force Protection Battle Lab
  - Surgeon General
- U.S. Army
  - 52nd Ordnance Group
  - Chemical School
  - Forces Command
  - Maneuver Support Center
  - Medical Research Institute for Infectious Diseases
  - National Ground Intelligence Center
  - Soldier and Biological Chemical Command
    - Edgewood Chemical Biological Center

  - Technical Escort Unit
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
  - Systems Command
- U.S. Navy
  - Naval Air Warfare Center
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Forces Central Command
  - Naval Surface Warfare Center
  - Office of Naval Research

U.S. Department of Energy
- National Nuclear Security Administration
  - Chemical and Biological National Security Program
- Office of Security

U.S. Department of Health and Human Services
- Centers for Disease Control and Prevention
- Food and Drug Administration
- Public Health Service
  - Office of Emergency Preparedness

U.S. Department of Justice
- Federal Bureau of Investigation
  - Bomb Data Center
  - Hazardous Materials Response Unit
  - Weapons of Mass Destruction Operations Unit
- Marshals Service
- National Institute of Justice

U.S. Department of State
- Bureau of Diplomatic Security
- Office of the Coordinator for Counterterrorism
- Overseas Building Operations

U.S. Department of the Treasury
- Customs Service
- Secret Service
  - Technical Security Division

U.S. Department of Transportation
- Coast Guard
- Transportation Security Administration

U.S. Postal Inspection Service

Washington Metropolitan Area Transit Authority, Transit Police Department

White House
- Office of Homeland Security
- Office of Science and Technology Policy

Explosives Detection

U.S. Capitol Police

U.S. Department of Defense
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Force Protection Systems Program Office
- Joint Chiefs of Staff
- Joint Services Explosive Ordnance Disposal
- National Security Agency
- U.S. Air Force
  - Air Combat Command
  - Force Protection Battle Lab
  - Research Lab
- U.S. Army
  - Technical Escort Unit
- U.S. Navy
  - Naval Criminal Investigation Service
  - Naval Explosive Ordnance Disposal Technology Division
  - Naval Facilities Engineering Service Center
  - Naval Surface Warfare Center
  - Research Laboratory

U.S. Department of Energy
- Office of Security

U.S. Department of Justice
- Federal Bureau of Investigation
  - Bomb Data Center
- National Institute of Justice

U.S. Department of State
- Bureau of Diplomatic Security

U.S. Department of the Treasury
- Bureau of Alcohol, Tobacco, and Firearms
- Customs Service
- Secret Service

U.S. Department of Transportation
- Coast Guard
- Transportation Security Administration

U.S. Postal Inspection Service

Improvised Device Defeat

Columbus Fire Department, Bomb Squad

District of Columbia Metropolitan Police Department, Bomb Squad

Fairfax County Police Department, Bomb Squad

Maricopa County Sheriff's Office, Bomb Squad

National Bomb Squad Commanders' Advisory Board

Prince George's County Fire Department, Bomb Squad

U.S. Capitol Police

U.S. Department of Defense
- Defense Intelligence Agency
- Force Protection Systems Program Office
- National Security Agency
- U.S. Air Force
  - Air Combat Command
  - Air Force Research Lab
- U.S. Army
- U.S. Navy
  - Naval Criminal Investigation Service
  - Naval Explosive Ordnance Disposal Technology Division

U.S. Department of Justice
- Federal Bureau of Investigation
  - Bomb Data Center
- National Institute of Justice

U.S. Department of the Treasury
- Bureau of Alcohol, Tobacco, and Firearms
- Customs Service
- Secret Service

U.S. Department of Transportation
- Transportation Security Administration

U.S. Postal Inspection Service

Infrastructure Protection

Environmental Protection Agency

Federal Emergency Management Agency

Nuclear Regulatory Commission

U.S. Department of Agriculture
- Forest Service

U.S. Department of Commerce
- Critical Infrastructure Assurance Office
- National Institute of Standards and Technology

U.S. Department of Defense
- Defense Threat Reduction Agency
- Joint Forces Command

- Joint Program Office, Special Technology Countermeasures
- U.S. Air Force
  - Office of Special Investigations
- U.S. Army
  - Computer Crimes Investigative Unit
  - Corps of Engineers
- U.S. Navy
  - Naval Criminal Investigation Service
  - Naval Surface Warfare Center

U.S. Department of Energy

U.S. Department of Justice
- Federal Bureau of Investigation
- National Infrastructure Protection Center

U.S. Department of the Treasury
- Secret Service

U.S. Department of Transportation
- Federal Aviation Administration

Investigative Support and Forensics

Environmental Protection Agency

Federal Emergency Management Agency

Intelligence Community

National Forensic Science Technology Center

U.S. Department of Commerce
- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

U.S. Department of Defense
- Armed Forces Institute of Pathology
- Defense Threat Reduction Agency
- Force Protection Systems Program Office
- National Security Agency
- Polygraph Institute
- U.S. Army
  - Criminal Investigation Command
- U.S. Marine Corps
  - Chemical Biological Incident Response Force
- U.S. Navy
  - Naval Criminal Investigation Service

U.S. Department of Justice
- Drug Enforcement Administration
- Federal Bureau of Investigation
  - National Center for Forensic Science
- Marshals Service
- National Institute of Justice

U.S. Department of the Treasury
- Bureau of Alcohol, Tobacco, and Firearms
- Customs Service
- Internal Revenue Service
- Secret Service

U.S. Department of Transportation
- Transportation Security Administration

U.S. Postal Inspection Service

U.S. Postal Service

Personnel Protection

U.S. Department of Commerce
- National Institute of Standards and Technology
  - Office of Law Enforcement Standards

U.S. Department of Defense
- U.S. Army
  - Natick Research, Development, and Engineering Center
  - Tank-Automotive and Armaments Command

U.S. Department of Energy
- Office of Security

U.S. Department of Justice
- National Institute of Justice

U.S. Department of Labor
- Office of the Inspector General

U.S. Department of State
- Bureau of Diplomatic Security

U.S. Department of the Treasury
- U.S. Secret Service
  - Special Services Division
  - Technical Security Division

Physical Security

Federal Emergency Management Agency

General Services Administration
- Federal Protection Service

Intelligence Community

Nuclear Regulatory Commission

Supreme Court of the United States

U.S. Department of Defense
- Central Command
- Defense Intelligence Agency
- Defense Logistics Agency
- Defense Threat Reduction Agency
- European Command
- Joint Chiefs of Staff
- Joint Forces Command
- National Reconnaissance Office
- National Security Agency
- Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
- Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics
- Pentagon Force Protection Agency
- Pacific Command
- U.S. Air Force
- U.S. Army
- U.S. Marine Corps
- U.S. Navy

U.S. Department of Energy
- National Nuclear Security Administration
- Office of Security

U.S. Department of Justice
- Federal Bureau of Prisons
- National Institute of Justice

U.S. Department of State
- Bureau of Diplomatic Security

U.S. Department of the Treasury
- Bureau of Alcohol, Tobacco, and Firearms
- Customs Service
- Federal Reserve Board
- Secret Service

U.S. Department of Transportation
- Coast Guard
- Office of Information Systems
- Transportation Security Administration

U.S. Postal Service

Surveillance, Collection and Operations Support

Intelligence Community

U.S. Department of Defense
- Defense Intelligence Agency
  - Central MASINT Organization
- National Reconnaissance Office
- National Security Agency
- Special Operations Command

U.S. Department of Justice
- Drug Enforcement Administration
- Federal Bureau of Investigation

U.S. Department of the Treasury
- Customs Service
- Secret Service

Tactical Operations Support

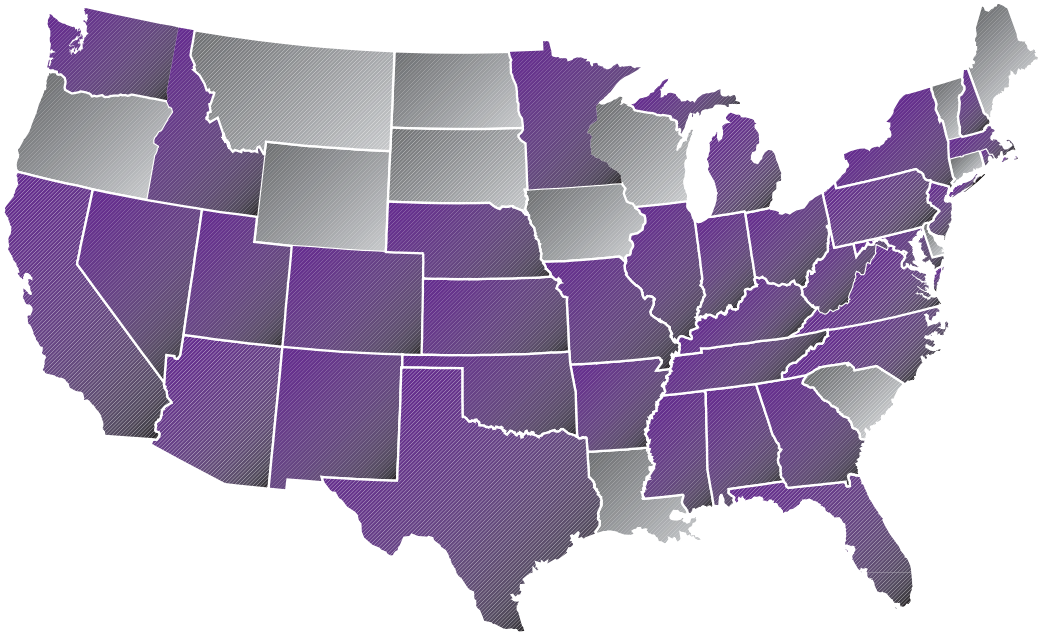
U.S. Department of Defense
- Special Operations Command

U.S. Department of Energy
- Office of Security

U.S. Department of Justice
- Federal Bureau of Investigation
  - Hostage Rescue Team

U.S. Department of the Treasury
- Secret Service

TSWG Performers



Alabama
Auburn University
Auburn University Institute for Biological Detection Systems
Missile and Space Intelligence Center

Arizona
Armorworks Corp.
Authenti-Corp.
Litton Electro-Optical Systems
Thunder Mountain Evaluation Center

Arkansas
Tekne Group, Inc.

California
3rd Ring
ACM Systems
Applied Signals Technology
Dynamics Technology Incorporated
Karagozian & Case
Lawrence Livermore National Laboratory
Maxim Systems, Inc.
Mission Research Corporation
Naval Facilities Engineering Command
Petrogen
Quantum Magnetics
San Jose State University
Science Applications International Corporation (SAIC)
SPAWAR Systems Center-San Diego
Special Technologies Laboratory
SRI International
University of California – Davis
Virage, Inc.

Colorado
Applied Research Associates

District of Columbia
U.S. Naval Research Laboratory

Florida
ANRO Engineering, Inc.
Florida International University
Harris Government Communications Systems Division
Knights Armament, Inc.
Megaseal Corp.
National Terrorism Preparedness Institute
Purified Micro Environments, Orlando
U.S. Air Force Civil Engineering Support Agency
U.S. Air Force Force Research Laboratory
University of Florida

Georgia
Georgia Tech Research Institute

Idaho
Idaho National Engineering and Environmental Laboratory

Illinois
Gas Technology Institute

Nanosphere

Indiana
Creative Building Products, Inc.

Golden Engineering

Naval Surface Warfare Center, Crane Division

Kansas
Midwest Research Institute

NanoScale Materiels

Kentucky
Western Kentucky University

Maryland
Atlantic Coast Technology

Eumetria, Inc.

GEOMET Technologies

Johns Hopkins University Applied Physics Laboratory

Johns Hopkins University Medical School

Lagus Applied Technology

Loats Associates

Multispectral Solutions, Inc.

National Institute of Standards and Technology

Naval Explosive Ordnance Disposal Technology Division

Naval Surface Warfare Center – Carderock

Perkin Elmer

Technology Service Corporation

U.S. Army Edgewood Chemical and Biological Center

University of Maryland/Food and Drug Administration

Massachusetts
BBN Technologies

Charles Stark Draper Lab

Curtiss Wright/Lau Defense Systems, Inc.

iRobot

Massachusetts Institute of Technology, Lincoln Laboratory

MITRE

Surmet

Technical Products, Inc.

TIAX, LLC

Tufts University

U.S. Air Force Electronics Systems Center

Viisage Technology

Volpe National Transportation Technical Center

Michigan
Triad Services Group

Wayne State University Bioengineering Center

Minnesota
Honeywell Laboratories

Mississippi
ProVision Technologies

U.S. Army Corps of Engineers, Engineering Research and Development Center, Waterways Experimental Station

Missouri
Clean Earth Technology

Nebraska
U.S. Army Corps of Engineers, Protective Design Center

University of Nebraska, Lincoln

Nevada
Bechtel – Remote Sensing Laboratory

Sparta, Inc.

University of Nevada, Las Vegas

New Hampshire
Impact Science and Technology

Wilcox Industries

New Jersey
Galaxy

Hi Temp Technology, Inc.

Picatinny Arsenal

Sarnoff Corporation

U.S. Army Communications Electronics Command (CECOM)

New Mexico
Applied Research Associates

New Mexico Tech Energetic Materials Research & Testing Center

Sandia National Laboratories

Science and Engineering Associates

New York
Ocean & Atmospheric Science, Inc.

Sensatex, Inc

Veridian Pacific-Sierra Research

Weidlinger Associates, Inc.

North Carolina
Research Triangle Insitute
Signalscape
Tempest Environmental Systems, Inc.

Ohio
Battelle Memorial Institute
Komar Industries, Inc.
Ohio University
University of Dayton Research Institute

Oklahoma
Nomadics

Pennsylvania
Carnegie Mellon University
Concurrent Technologies Corp.
Early Responders Distance Learning Center, St. Joseph's University
Franklin Applied Physics
Indiana University of Pennsylvania
Optical Systems Technology, Inc.
University of Pittsburgh

Rhode Island
University of Rhode Island

Tennessee
British Aerospace Engineering Systems, Ordnance Systems Inc
Northrop Grumman REMOTEC
PIPS Technology

Texas
Applied Research Associates
BAE Systems
EQE International
Northrup Grumman-Litton Electro Optical Systems
Southwest Research Institute
U.S. Air Force Force Protection Battlelab
U.S. Army Institute of Surgical Research
University of Texas, Austin
Wilfred Baker Engineering, Inc.

Utah
Mission Research Corporation
Utah State University

Virginia
Applied Marine Technology, Inc.
Autometric, Inc.
Battelle Memorial Institute
Booz·Allen & Hamilton
Defense Threat Reduction Agency
Galaxy Scientific
General Testing Laboratories
Naval Surface Warfare Center, Dahlgren Division
ORION Scientific Systems
QinetiQ
Science Applications International Corporation (SAIC)
SRA International, Inc.
Tetratech, Inc.
The Bode Technology Group
U. S. Army Night Vision & Electronic Sensors Directorate
U.S. Army Product Manager for Physical Security Equipment
U.S. Army Software Engineering Center
Veridian Engineering Systems, Inc.
Veridian Information Systems, Inc.

Washington
Pacific Northwest National Laboratory
Washington State University

West Virginia
West Virginia University

International Partners

Australia
Queensland University of Technology, Brisbane

Canada
Defence Research Establishment
EOD Performance
MREL

Israel
Israel Institute for Biological Research
Israel Security Agency
Israeli National Police
Ministry of Defense

United Kingdom
Defence Science and Technology Laboratories
Forensic Science Service
Police Scientific Development Branch

Glossary of Acronyms

A

ACC	Air Combat Command
AFB	Air Force Base
AFOSI	Air Force Office of Special Investigations
AFRL	Air Force Research Lab
AMRIID	Army Medical Research Institute for Infectious Diseases
APHIS	Animal and Plant Health Inspection Service
APV	Armored Personnel Vehicle
ARS	Agricultural Research Service
ASD(SO/LIC)	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
ASDE	Airport Surface Detection Equipment
ASDP	Airport Security Display Processor
ATF	Bureau of Alcohol, Tobacco, and Firearms
AT-Planner	Anti-Terrorism Planner
ATrCT	Alert Trend Change Tool
AVIDS	Advanced Vehicle Driver Identification System

B

BAA	Broad Agency Announcement
BCJOC	Biological Chemical Joint Operations Center
BEEM	Blast Effects Estimation Model
BIDS	BAA Information Delivery System

C

C^4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CBIRF	Chemical Biological Incident Response Force
CBNP	Chemical and Biological National Security Program
CBR	Chemical, Biological, and Radiological
CBRN	Chemical, Biological, Radiological and Nuclear
CDC	Centers for Disease Control and Prevention
CENTCOM	Central Command
CIAO	Critical Infrastructure Assurance Office
CIDC	Army Criminal Investigation Command
CIRTS	Critical Incident Response Training Seminars
CoBRA™	Chemical/Biological Response Aide
CTTS	Combating Terrorism Technology Support
CWA	Chemical Warfare Agent

D

DARPA	Defense Advanced Research Projects Agency
DEA	Drug Enforcement Administration
DGPS	Differential GPS-based
DIA	Defense Intelligence Agency
DIA/CMO	Defense Intelligence Agency – Central MASINT Organization
DLA	Defense Logistics Agency

DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DoDPI	Department of Defense Polygraph Institute
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
DOT	Department of Transportation
DPS	Defense Protective Service
DS	Bureau of Diplomatic Security
DTRA	Defense Threat Reduction Agency

E

ECBC	Edgewood Chemical Biological Center
ED	Explosives Detection
EOD	Explosive Ordnance Disposal
EPA	Environmental Protection Agency
EUCOM	European Command

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FBI-BDC	Federal Bureau of Investigation Bomb Data Center
FBI-HRT	Federal Bureau of Investigation Hostage Rescue Team
FBOP	Federal Bureau of Prisons
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FLIR	Forward Looking Infrared
FPBL	Force Protection Battlelab
FPS	Federal Protective Services
FPSPO	Force Protection Systems Program Office
FPT	Force Protection Tool
FRB	Federal Reserve Board
FS	Forest Service
FSIS	Food Safety and Inspection Service
FY	Fiscal Year

H

HAZMAT	Hazardous Materials
HMRU	Hazardous Materials Response Unit

I

IAB	InterAgency Board for Equipment Standardization and InterOperability
IC	Intelligence Community
IDD	Improvised Device Defeat
IED	Improvised Explosive Device
IG/T	Interdepartmental Working Group on Terrorism
INS	Immigration and Naturalization Service
IO	Information Operations
IP	Infrastructure Protection

IR	Infrared
IRS	Internal Revenue Service
IS&F	Investigative Support and Forensics
IWG/CT	Interagency Working Group on Counterterrorism

J

JCS	Joint Chiefs of Staff
JFCOM	Joint Forces Command
JPO-STC	Joint Program Office-Special Technology Countermeasures

L

LAN	Local Area Network
LLNL	Lawrence Livermore National Laboratory
LVB	Large Vehicle Bomb

M

MANSCEN	Maneuver Support Center
MIT	Massachusetts Institute of Technology
MMVACIS	Military Mobile Vehicle and Cargo Inspection System

N

NATO	North Atlantic Treaty Organization
NAVCENT	Navy Forces Central Command
NAVEODTECHDIV	Naval Explosive Ordnance Disposal Technology Division
NAWC	Naval Air Warfare Center
NCFS	National Center for Forensics Science
NCIS	Naval Criminal Investigation Service
NFESC	Naval Facilities Engineering Service Center
NGIC	National Ground Intelligence Center
NIJ	National Institute of Justice
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
NIST-OLES	National Institute of Standards and Technology Office of Law Enforcement Standards
NNSA	National Nuclear Security Administration
NRL	Naval Research Laboratory
NRO	National Reconnaissance Office
NSA	National Security Agency
NSDD	National Security Decision Directive
NSWC	Naval Surface Warfare Center

O

OASD(C^3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
OATSD/CBD	Office of the Assistant to the Secretary of Defense/Chemical and Biological Defense
OBO	Overseas Building Operations
OEP	Office of Emergency Preparedness
OIC	Officer in Charge
OIG	Office of the Inspector General
OIS	Office of Information Systems

ONR	Office for Naval Research
OS	Office of Security
OSTP	Office of Science and Technology Policy
OUSD(AT&L)	Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics

P

PACOM	Pacific Command
PAPR	Powered Air Purifying Respirator
PELAN	Pulsed Elemental Analysis with Neutrons
PFPA	Pentagon Force Protection Agency
PipelineNet	Pipeline Network Modeling System
PP	Personnel Protection
PS	Physical Security

Q

QR	Quadrupole Resonance
QUPID	Quick Reaction Perimeter Intrusion Detection Sensor

R

R&D	Research and Development
RAID	Redundant Array of Independent Disks
RAM-D	Risk Assessment Methodology for Dams
RD&E	Research, Development, and Engineering
REALITI	Response Element Advanced Laboratory Integrated Training and Indoctrination
RF	Radio-Frequency
RiverSpill	Real Time River Spill System

S

S/CT	Department of State Office of the Coordinator for Counterterrorism
SAST	Systems Administrator Simulation Trainer
SAW	Surface Acoustic Wave
SBCCOM	Soldier and Biological Chemical Command
SC&OS	Surveillance, Collection and Operations Support
SCADA	Supervisory Control and Data Acquisition
SCBA	Self-contained breathing apparatus
SG	Surgeon General
SO/LIC	Special Operations and Low-Intensity Conflict
SOCOM	Special Operations Command
SOP	Standard Operating Procedure
STU	Secure Telephonic Unit

T

TACOM	Tank-Automotive and Armaments Command
TATP	Triacetone Triperoxide
TEU	Technical Escort Unit
TIC	Toxic Industrial Chemical
TNT	Trinitrotoluene
TOS	Tactical Operations Support

TSA	Transportation Security Administration
TSWG	Technical Support Working Group
TTL	Tagging, Tracking, And Locating

U

USA	United States Army
USACE	United States Army Corps of Engineers
USACMLS	United States Army Chemical School
USAF	United States Air Force
USCG	United States Coast Guard
USCS	United States Customs Service
USDA	United States Department of Agriculture
USMC	United States Marine Corps
USMS	United States Marshals Service
USN	United States Navy
USPHS	United States Public Health Service
USPS	United States Postal Service
USSS	United States Secret Service
USSS-SSD	United States Secret Service – Special Services Division
USSS-TSD	United States Secret Service – Technical Security Division
UV	Ultraviolet

V

VIP	Very Important Person
VIPS	Vessel Identification and Positioning System

W

WAN	Wide Area Network
WMD	Weapons of Mass Destruction
WMDOU	Weapons of Mass Destruction Operations Unit